Figure 3: The distribution of inter-keystroke timings for two sample character pairs.
Figure 5: Estimated Gaussian distributions of all 142 character pairs collected from a user.
Figure 8 graphs the probability that the real character pair appears within the $n$ most-likely character pairs against the threshold $n$. 

Figure 8: The probability that the $n$-Viterbi algorithm outputs the correct password before the first $n$ guesses, graphed as a function of $n$. 
Figure 10: The percentage of the password space tried by Herbivore in 10 tests before finding the right password.
**IP Header Side Channel**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>4-bit Version</strong></td>
<td>Version of the IP protocol version.</td>
</tr>
<tr>
<td><strong>4-bit Header Length</strong></td>
<td>Length of the IP header in bytes.</td>
</tr>
<tr>
<td><strong>8-bit Type of Service (TOS)</strong></td>
<td>Type of Service (TOS).</td>
</tr>
<tr>
<td><strong>16-bit Total Length (Bytes)</strong></td>
<td>Total length in bytes.</td>
</tr>
<tr>
<td><strong>16-bit Identification</strong></td>
<td>Identification field.</td>
</tr>
<tr>
<td><strong>3-bit Flags</strong></td>
<td>Flags used for fragmentation.</td>
</tr>
<tr>
<td><strong>13-bit Fragment Offset</strong></td>
<td>Offset for segment.</td>
</tr>
<tr>
<td><strong>8-bit Time to Live (TTL)</strong></td>
<td>Time to Live (TTL).</td>
</tr>
<tr>
<td><strong>8-bit Protocol</strong></td>
<td>Protocol number of the upper layer.</td>
</tr>
<tr>
<td><strong>16-bit Header Checksum</strong></td>
<td>Header checksum.</td>
</tr>
<tr>
<td><strong>32-bit Source IP Address</strong></td>
<td>Source IP Address.</td>
</tr>
<tr>
<td><strong>32-bit Destination IP Address</strong></td>
<td>Destination IP Address.</td>
</tr>
<tr>
<td><strong>Payload</strong></td>
<td>Data portion of the IP packet.</td>
</tr>
</tbody>
</table>

ID field is supposed to be unique per IP packet.

One easy way to do this: **increment** it each time system sends a new packet.
**Attacker**

Echo request

reply, ID=3

**Patsy**

**Victim**
SYN-ACK
Attacker

Echo request
reply, ID=3

Echo request
reply, ID=4

Echo request
reply, ID=5

TCP SYN, src=P, dst port=24

Patsy

Victim
Attacker  →  Patsy  →  Victim

- Echo request  
  reply, ID=3
- Echo request  
  reply, ID=4
- Echo request  
  reply, ID=5
- TCP SYN, src=P, dst_port=24

Spoofed
**Attacker**

- Echo request
  - reply, ID=3

+1

- Echo request
  - reply, ID=4

+1

- Echo request
  - reply, ID=5

TCP SYN, src=P, dst port=24

**Patsy**

**Victim**

no listener on port 24, RST generated
Upon receiving RST, Patsy ignores it and does **nothing**, per TCP spec.
Attacker

- Echo request
- Echo request
- Echo request
- TCP SYN, src=P, dst port=24
- Echo request

Patsy

- reply, ID=3
- reply, ID=4
- reply, ID=5
- TCP RST

- reply, ID=6

no listener

Victim

no listener on port 24, RST generated
Spoofed

Listener exists on port 25, SYN-ACK generated.

Attacker

TCP SYN, src=P, dst port=25
reply, ID=7
Echo request

TCP SYN-ACK

no listener on port 24, RST generated.

Victim

Attacker

TCP SYN, src=P, dst port=24
reply, ID=5
Echo request

TCP SYN-ACK

no listener on port 24, RST generated.

Victim

TCP SYN-ACK

no listener on port 25, RST generated.
Attacker | Patsy | Victim
---|---|---
- Echo request reply, ID=3
- Echo request reply, ID=4
- Echo request reply, ID=5
- TCP SYN, src=P, dst port=24
- Echo request reply, ID=6
- Echo request reply, ID=7
- TCP SYN, src=P, dst port=25
- TCP SYN-ACK
- TCP RST, ID=8

no listener on port 24, RST generated

no listener exists on port 25, SYN-ACK generated.

P has no state for this connection, so generates a RST, which increments the IP ID sequence.
**Attacker**

- Echo request, reply, ID=3
- Echo request, reply, ID=4
- Echo request, reply, ID=5
- TCP SYN, src=P, dst port=24
- TCP RST
- Echo request, reply, ID=6
- Echo request, reply, ID=7
- TCP SYN, src=P, dst port=25
- TCP SYN-ACK
- TCP RST, ID=8
- Echo request, reply, ID=9
- Echo request, reply, ID=10

**Patsy**

- no listener on port 24, RST generated

**Victim**

- listener exists on port 25, SYN-ACK generated.

*P has no state for this connection, so generates a RST, which increments the IP ID sequence.*
Order approved

Your transaction has been approved.

Your order ID: 138730
First name: Geoff
Last name: Voelker
Card used with this order: 46****2205
Total amount charged: $64.95

The following billing descriptor appear on your credit card statement:

medissue.com +12175686119

Tracking number will be sent on your email once medications will be shipped.

NOTE: Contact us about your order only through customers support system www.rxsup24.com
Before contact us and ask about time for delivery please read our shipping policy.

ORDER STATUS, TRACKING NUMBER, FAQ ABOUT DELIVERY:

Website menu --> Order status

Dear Geoff Voelker, if you have any questions regarding your order, shipping, please contact us at:

Customers support system: www.rxsup24.com
Order approved

Your transaction has been approved.

Your order ID: 138731
First name: Kirill
Last name: Levchenko
Card used with this order: 46****2288
Total amount charged: $52.95

The following billing descriptor appear on your credit card statement:
 =================
medisssue.com +12175686119
 =================

Tracking number will be sent on your email once medications will be shipped.

NOTE: Contact us about your order only through customers support system www.rxsup24.com
Before contact us and ask about time for delivery please read our shipping policy.

ORDER STATUS, TRACKING NUMBER, FAQ ABOUT DELIVERY:

Website menu --> Order status

Dear Kirill Levchenko, if you have any questions regarding your order, shipping, please contact us at:

Customers support system: www.rxsup24.com
Order approved

Your transaction has been approved.

Your order ID: 138730
First name: Geoff
Last name: Voelker
Card used with this order: 46*****2205
Total amount charged: $64.95

The following billing descriptor appear on your credit card statement:

medissue.com +12175686119

Tracking number will be sent on your email once medications will be shipped.

NOTE: Contact us about your order only through customers support system www.rxsup24.com
Before contact us and ask about time for delivery please read our shipping policy.

ORDER STATUS, TRACKING NUMBER, FAQ ABOUT DELIVERY:

Website menu --> Order status

Dear Geoff Voelker, if you have any questions regarding your order, shipping, please contact us at:

Customers support system: www.rxsup24.com
Order approved

Your transaction has been approved.

Your order ID: 138731
First name: Kirill
Last name: Levchenko
Card used with this order: 46*****2288
Total amount charged: $52.95

The following billing descriptor appear on your credit card statement:

medisssue.com +12175686119

Tracking number will be sent on your email once medications will be shipped.

NOTE: Contact us about your order only through customers support system www.rxsup24.com
Before contact us and ask about time for delivery please read our shipping policy.

ORDER STATUS, TRACKING NUMBER, FAQ ABOUT DELIVERY:

Website menu --> Order status

Dear Kirill Levchenko, if you have any questions regarding your order, shipping, please contact us at:

Customers support system: www.rxsup24.com
Order approved

Your transaction has been approved.

Your order ID: 144571
First name: Geoff
Last name: Voelker
Card used with this order: 46****4029
Total amount charged: $64.95

The following billing descriptor appear on your credit card statement:

medissue.com +12175686119

Tracking number will be sent on your email once medications will be shipped.

NOTE: Contact us about your order only through customers support system www.rxsup24.com
Before contact us and ask about time for delivery please read our shipping policy.

ORDER STATUS, TRACKING NUMBER, FAQ ABOUT DELIVERY:

Website menu --> Order status

Dear Geoff Voelker, if you have any questions regarding your order, shipping, please contact us at:

Customers support system: www.rxsup24.com
A diagram illustrates a affiliate program where users make purchases, earning affiliate fees. There are $N$ other purchases, with one being our purchase marked with 4200 and 4224. The affiliate program connects to an order database with order IDs 4200, 4201, ..., 4224. The total number of orders is denoted as $N=23$. The diagram emphasizes the flow of purchases and the earnings through the affiliate program.
If orders are timer-driven, expect a narrow range of timing errors reflecting batch size.

If skewed by outliers, expect an up/down or down/up trend around the outlier.

If orders not timer-driven, then we just see residuals with respect to the underlying order rate. ⇒ should have a cloud of points.